03-10-00

A

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Raivisto

Serial No. TO BE ASSIGNED

Corresponding to PCT/FI98/00720, filed 15 September 1998

Filed: 9 March 2000 Docket No.: 796.337USW1

Title: SECURITY METHOD FOR TRANSMISSIONS IN TELECOMMUNICATION NETWORKS

CERTIFICATE UNDER 37 C.F.R. 1.10:
'Express Mail' mailing number: EL477365502US
Date of Deposit: 9 March 2000
The undersigned hereby certifies that this Transmittal Letter and the paper or fee, as described herein, are being deposited with the United States Postal Service 'Express Mail Post Office To Addressee' service under 37 CFR 1.10 and is addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231

By: Theresa Jurek

Box Patent Application
Assistant Commissioner for Patents
Washington, D.C. 20231

REQUEST FOR CONTINUATION OF AN INTERNATIONAL APPLICATION UNDER 37 C.F.R. §1.53(b)

This is a request for filing a continuation application under 37 C.F.R. §1.53(b) of prior pending international application number PCT/FI98/00720 filed on 15 September 1998 entitled SECURITY METHOD FOR TRANSMISSIONS IN TELECOMMUNICATION NETWORKS,which designated the United States.

1. ☒ Enclosed is a patent application containing 7 pages of specification, 8 claims and 2 sheet(s) of drawings.

2. ☒ A preliminary amendment is enclosed.

3. ☒ Please amend the specification by inserting the following paragraph after the title:

   This application is a continuation of international application serial number PCT/FI98/00720, filed 15 September 1998.

4. ☐ Small entity status
   a. ☐ A small entity statement is enclosed.
   b. ☐ A small entity statement was filed in the prior non provisional application.
   c. ☐ is no longer claimed.

The filing fee is calculated below

CLAIMS				
	Number Filed	Number Extra	Rate	Fee
Total Claims	8	0	X $18.00	$
Indep. Claims	1	0	X $78.00	$
Multiply Dependent Claims				$
			Basic Fee	$ 690.00
			TOTAL	$ 690.00

5. ☒ Payment of filing fees
   - ☐ A check in the amount of is enclosed.
   - ☐ Please charge Deposit Account Number 50-1038.
   - ☒ Is deferred.

6. ☒ The Commissioner is hereby authorized to credit any overpayment or charge any fees required under 37 C.F.R. §1.16-1.18 to Deposit Account Number 50-1038.

7. ☒ The priority of Finnish application number 973694, filed 15 September 1997, is claimed under
   35 U.S.C. §119.

8. ☒ A unsigned Declaration is enclosed.

9. ☐ An assignment of the invention to , Recordation Form Cover Sheet (Patents Only) and a check in the amount of $40.

10. ☒ An Information Disclosure Statement, Form PTO 1449 and copies of 4 citations are enclosed.

11. ☒ Correspondence Address

Altera Law Group
10749 Bren Road East
Minneapolis, Minnesota 55343

12. ☒ Address all correspondence to Michael B. Lasky.

13. ☒ Also enclosed: International Search Report for PCT/FI98/00720

14. ☒ A return postcard is enclosed.

Respectfully submitted,

ALTERA LAW GROUP, LLC
10749 Bren Road East
Minneapolis, MN 55343-9056

Dated: 9 March 2000

Michael B. Lasky
Atty. Reg. Number 29,555
MBL/mka

S/N UNKNOWN PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Raivisto	Serial No.:	UNKNOWN
Filed:	CONCURRENT HEREWITH	Docket No.:	796.337USW1
Title:	SECURITY METHOD FOR TRANSMISSIONS IN TELECOMMUNICATION NETWORKS		

CERTIFICATE UNDER 37 CFR 1.10
'Express Mail' mailing label number: EL477365502US
Date of Deposit: 9 March 2000
I hereby certify that this correspondence is being deposited with the United States Postal Service 'Express Mail Post Office To Addressee' service under 37 CFR 1.10 on the date indicated above and is addressed to the Assistant Commissioner for Patents, Washington, D.C . 20231.

By: Theresa Jurek
Name: Theresa Jurek

PRELIMINARY AMENDMENT

Box Patent Application
Assistant Commissioner for Patents
Washington, D.C. 20231

Dear Sir:

Please enter the following preliminary amendment into the above-referenced application.

ABSTRACT

Please insert the attached abstract into the application as the last page thereof.

CLAIMS

Please amend the claims as follows:

In claim 5, line 1, please remove “or 4”.

REMARKS

The above preliminary amendment is made to insert an abstract page into the application and to remove multiple dependencies from claim 4.

Applicant respectfully requests that this preliminary amendment be entered into the record prior to calculation of the filing fee and prior to examination and consideration of the above-identified application.

If a telephone conference would be helpful in resolving any issues concerning this communication, please contact Applicant's attorney of record, Michael B. Lasky at (612) 912-0527.

Respectfully submitted,

ALTERA LAW GROUP, LLC
10749 Bren Road East
Minneapolis, MN 55343-9056

Dated: 9 March 2000

Michael B. Lasky
Atty. Reg. Number 29,555
MBL/mka

Security method for transmissions in telecommunication networks

Field of the invention

The invention relates to a method for providing connection security for transmission between the communicating parties in a telecommunication network.

Background of the invention

At the beginning of a communication a handshake is usually performed between applications in telecommunication networks, during which the parties involved typically authenticate each other and exchange key information, for example, negotiate an encryption algorithm and cryptographic keys to be used in communication. It is only after the handshake that the actual data is transmitted. The confidentiality of the transmission is arranged, for example, through ciphering. Figures 1a and 1b of the attached drawings show block diagrams of two known cipher algorithms which can be used to protect a transmission: a symmetric and a public key algorithm.

Figure 1a shows a symmetric algorithm based on a secret key shared between the participants. At party A's end the message M to be sent to party B is encrypted in box E of Figure 1a with the shared secret key K. The message is sent over a transmission route as encrypted cipher text C, which party B can decrypt in box D shown in Figure 1a with the same secret key K. Through decryption party B gets the original message M. An intruder eavesdropping transmission needs to know the secret key K in order to be able to read and understand the transmitted cipher text C. The encryption and decryption of the symmetric algorithm can be expressed by the equations:

$$C = E_K(M)$$

$$M = D_K(C),$$

where C is the cipher text, M is the message in plain text, E_K is the encryption with key K, and D_K is the decryption with key K.

Figure 1b shows a public key algorithm which is an asymmetric approach. This algorithm is based on two keys: a public key and a private key. These two keys are related in such a manner that a message encrypted with a public key K_+ can only be decrypted with the corresponding private key K_- and vice versa. In Figure 1b a message M is encrypted at party A's end in

box E with the public key K_+ of the intended receiver, that is party B. The encrypted cipher text C is transmitted over a transmission line to party B's end, where the cipher text C is decrypted in box D with the corresponding party B's private key K_- and the original message M is retrieved. The encryption and decryption of the asymmetric algorithm can also be expressed by the following equations:

$$C = E_B^+(M)$$

$$M = D_B^-(C),$$

where C is the cipher text, M is the message in plain text, E_B^+ is encryption with the receiver's public key K_B^+, and D_B^- is decryption with the receiver's private key K_B^-.

In the public key algorithm the encryption of a message with the private key K_- of the message sender acts as a signature, since anyone can decrypt the message with the known public key K_+ of the sender. Since asymmetric keys are usually much longer than symmetric keys, the asymmetric algorithm requires much more processing power. Thus asymmetric algorithms are unsuitable for encrypting large amounts of data.

A hybrid cryptography uses both the above-mentioned algorithms together. For example, only session keys are exchanged using public key algorithm, and the rest of the communication is encrypted with symmetric method.

To provide message integrity and authentication in a connection, a message authentication code MAC is calculated and attached to the transmitted message. For example, MAC can be calculated with a one-way hash algorithm in the following way:

$$h = H(K, M, K),$$

where K is the key, M is the message, and H is the hash function. The input cannot be deduced from the output. When MAC is attached to a message, the message cannot be corrupted or impersonated. The receiving party calculates MAC using the received message and the same hash function and key as the transmitting party and compares this calculated MAC to the MAC attached to the message in order to verify it.

Figure 2 shows examples for communication connections. A mobile station MS operating in the GSM network (Global System for Mobile communications) is able to make a connection to a bank directly from the GSM net-

work. Other possible connections presented in Figure 2 are connections from the GSM network to different services via gateway GW and Internet. In mobile communication networks, such as the GSM, the air interface from the mobile station MS to the GSM network is well protected against misuse, but the rest of the transmission route is as vulnerable as any other public telephone network, providing measures are not taken to provide connection security.

One problem with providing connection security is that handshaking requires plenty of processing time since several messages must be sent between the parties involved. The low processing power and narrow bandwidth in the mobile stations make handshakes particularly burdensome in mobile communication networks. Handshakes are also burdensome for applications which have numerous simultaneous transactions, for example, a server in a bank. Therefore, it is desirable to minimize the number and duration of the handshakes. This leads to the problem that an attacker has lots of time for cryptanalysis, as the same encryption keys are used between the two handshakes. If the attacker succeeds in the cryptanalysis, he can access all the material sent between the two handshakes.

Summary of the invention

The object of this invention is to provide a method for securely protecting transmitted information between communicating applications, especially over narrow-band connections, without unnecessarily loading the communicating parties.

This is achieved by using a method according to the invention characterized by what is stated in the independent claim 1. Special embodiments of the invention are presented in the dependent claims.

The invention is based on the idea that the communicating parties recalculate the security parameters during the transmission session simultaneously with each other at agreed intervals and the continue communicating and providing connection security for messages with these new parameters. The communicating parties monitor the time for recalculation and at the agreed intervals recalculate and thus change the security parameters without a handshake taking place. In the primary embodiment of the invention, the messages are numbered and the number agreed on triggers recalculation at intervals.

The advantage of the method according to the invention is that security parameters can be changed during the session without handshaking. This reduces the need for handshakes.

Another advantage of the method according to the invention is that the security of the transmission is improved, i.e. attacking is made more difficult and less profitable.

Brief description of the drawings

The description of the preferred embodiments of the invention will now be made with reference to the attached drawings, in which

Figure 1a shows a symmetric ciphering algorithm as a block diagram;

Figure 1b shows an asymmetric ciphering algorithm as a block diagram;

Figure 2 gives a few examples of connections from a mobile communication network to some applications;

Figure 3 shows session keys providing connection security for transmitted messages according to the primary embodiment of the invention; and

Figure 4 shows the primary embodiment of the invention as a flowchart.

Detailed description of the invention

The present invention can be applied to any telecommunication network. Below the invention is described in more detail using as an example a mobile station operating in the digital GSM mobile communication system and communicating with an application located either inside or outside the GSM network.

In the following the primary embodiment of the invention is described in more detail with reference to Figures 2, 3 and 4.

Figure 2 shows example connections as described earlier. The mobile station MS contacting the server in the bank first performs a handshake according to the prior art, during which both the MS and the bank may authenticate the other and exchange any session key information needed. According to the invention, for example, during the handshake, a mobile station and an application in the bank negotiate and agree on appropriate intervals for recalculating the security parameters to be used to provide privacy, data integrity and authentication during the communication. For example, the negotiation can be implemented so that each of the communicating parties,

i.e. in the example in Figure 2 the mobile station MS and the application in the bank, propose a suitable interval for recalculation and one of the proposed intervals is chosen and agreed upon, for example, the one that is more frequent. Examples for suitable parameters to determine intervals are a message sequence number, such as every fourth message, or a suitable time period. Even if handshaking is not needed and therefore not performed at the beginning of the communication session, according to the invention the communicating parties still need to agree on recalculation intervals.

After agreeing on the intervals for recalculation both the parties monitor the agreed intervals. If an interval after four messages is agreed on, either both parties monitor the number of messages sent, which requires a reliable transmission media with no lost messages, or they number all transmitted messages and transmit these sequence numbers with the messages. The advantage of sending the sequence numbers or time stamps with the messages is that the recalculation is synchronous at both ends even though some messages get lost along the way or messages received are not in correct order. When in the example described above the fourth message is transmitted and received, both the communicating parties recalculate the security parameters and use these new parameters for providing connection security for the next four messages. A handshake or any other session key exchange is not performed during or after the recalculation of the parameters. The recalculation can be based on a shared secret and the latest sequence number, for example. Security parameters can also be used to calculate session keys Kn for ciphering and the message authentication code MAC in the following way, for example:

Kn = H(S, N)

MAC = H(M, S, N),

where H is a predetermined hash algorithm, S is the shared secret, N is the latest sequence number, and M is the message to be transmitted in plain text.

Figure 3 shows an example of changing the session key according to the invention. In Figure 3 the messages sent from the MS are numbered with the sequence numbers 0 to 3. In the example in Figure 3, the interval for recalculation is agreed to be after two sent messages. The message with sequence number 0 is sent to the bank encrypted with session key K1. The application in the bank decrypts the message 0 with the same session key

K1 when symmetric algorithm is applied in ciphering. The message with sequence number 1 is also sent encrypted with session key K1. As the mobile station MS has now sent two messages, both the MS and the application in the bank recalculate the security parameters, for example, the session key K2, using the shared secret and the latest sequence number that is 1. After recalculation the MS sends the next message 2 to the bank encrypted with session key K2. The application in the bank decrypts the message 2 with the same recalculated session key K2. Also the message 3 is encrypted with session key K2 before transmission. After that the MS and the application in the bank again notice that the agreed interval has been reached and both parties recalculate the security parameters, for example, the session key K3, using the shared secret and the latest sequence number 3.

Figure 4 shows the primary embodiment of the invention as a flowchart. At the beginning of a communication at step 41, the parties involved in communication, in the example in Figure 2 the MS and the application in the bank, negotiate and agree on the interval for security parameters recalculation. As in the example described above, we again assume that the interval is agreed to be after two transmitted messages. Both communicating parties keep track of the number of transmitted messages, for example, with counters at each end. At stage 42 one of the communicating parties, for example, the MS, encrypts the first message to be sent with a session key K1 obtained from the shared secret that was exchanged during the handshake or otherwise shared with the parties involved. The encrypted message is sent and the receiving party decrypts the message with corresponding session key K1 (stage 43). At this time the counter is set at 1. At stage 44 both parties, in this example the MS and the application in the bank, check whether the agreed interval has been reached by checking whether the value in the counter is equal to the value of the agreed interval, for example. As the message sent was only the first message, recalculation does not take place yet, and the next message is encrypted and decrypted with the same session key K1. When two messages have been sent, and the counters indicate the value 2 which corresponds to the value of the agreed interval, the clause at stage 44 becomes true and both communicating parties recalculate security parameters in a predetermined manner and obtain a new session key K2 (stage 45). At stage 46 the interval monitoring is reset, i.e. the message count is restarted, for example, by setting the counter to 0. At stage 47 a

check is made as to whether there are still more messages to be sent, and if so the encryption of a message is continued at stage 42 with the first message to be encrypted using the latest session key K2, after which the message is sent and the counters may be set to value 1. The process continues in similar manner until all the messages to be sent are transmitted.

In another embodiment of the invention, MAC is used to provide connection security for message transmission in the place of ciphering. According to the invention MAC is calculated, from the sequence number that last triggered recalculation of the security parameters, for example. In the example in Figure 3, MAC is calculated with the sequence number 1 for the messages shown as encrypted with K2 and with the sequence number 3 for the messages to be encrypted with K3. Otherwise this other embodiment of the invention is implemented in the same fashion as in the first embodiment described above.

Yet another embodiment of the invention uses ciphering and MAC to provide connection security for messages. This is implemented by combining the embodiments described above.

Recalculation of the security parameters includes also the possibility of changing the ciphering algorithm to be used in ciphering the next messages.

The drawings and the accompanying explanation are only intended to demonstrate the principles of the invention. The details of the method according to the invention can vary within the patent claims. Although the invention was described above mostly in connection with a mobile station and service application communication, the invention can also be used for providing connection security for messages between any two or more applications communicating together, also in mobile to mobile connection in a speech, data and short message transmission. The invention is also suitable for use in recalculating other security parameters than session keys and MACs. The invention is not restricted for use only in connection with the ciphering algorithms presented above, but can be applied together with any ciphering algorithms.

Claims

1. Method for providing connection security for the transmission between communicating parties in a telecommunication network, the method comprising the steps of:

exchanging security parameters between communicating parties,

providing connection security for messages based on these security parameters, and

transmitting said messages between communicating parties,

characterized in that the method further comprises the steps of:

reaching agreement between communicating parties on an interval for recalculation of the security parameters,

monitoring of the interval for recalculation by the communicating parties,

recalculating the security parameters at the agreed interval, and

providing connection security for messages based on the latest recalculated security parameters.

2. Method according to claim 1, characterized in that providing connection security for messages based on the latest recalculated security parameters comprises the step of

ciphering messages based on the latest recalculated security parameters.

3. Method according to claim 1, characterized in that providing connection security for messages based on the latest recalculated security parameters comprises the step of

authenticating and providing integrity for the messages based on the latest recalculated security parameters.

4. Method according to claim 1, characterized in that providing connection security for messages based on the latest recalculated security parameters comprises the steps of

ciphering messages based on the latest recalculated security parameters, and

authenticating and providing integrity for the messages based on the latest recalculated security parameters.

5. Method according to claim 3 or 4, characterized in that authenticating and providing integrity for the messages is arranged with a message authentication code MAC.

6. Method according to claim 1, characterized in that the method further comprises the steps of:

numbering the messages,

agreeing on the number of messages to determine the interval for the recalculation of the security parameters,

recalculating the security parameters after the agreed number of messages have been transmitted.

7. Method according to claim 6, characterized in that the method further comprises the steps of:

numbering the messages with sequence numbers,

transmitting the sequence number with the message, and

using the latest sequence number as input for recalculation of the security parameters.

8. Method according to claim 1, characterized in that the method comprises the step of

reaching agreement between communicating parties during hand-shaking on the interval for recalculation of the security parameters.

ABSTRACT

SECURITY METHOD FOR TRANSMISSIONS IN TELECOMMUNICATION NETWORKS

The invention related to method for providing connection security for the transmission between communicating parties in a telecommunication network, the method comprising the steps of : exchanging security parameters between communicating parties, providing connection security for messages based on these security parameters, and transmitting said messages between communicating parties. It is characteristic for the method according to the invention that it further comprises the steps of: reaching agreement between communicating parties on an interval for recalculation of the security parameters, monitoring of the interval for recalculation by the communicating parties, recalculating the security parameters at the agreed interval, and providing connection security for messages based on the latest recalculated security parameters.

Fig. 1a

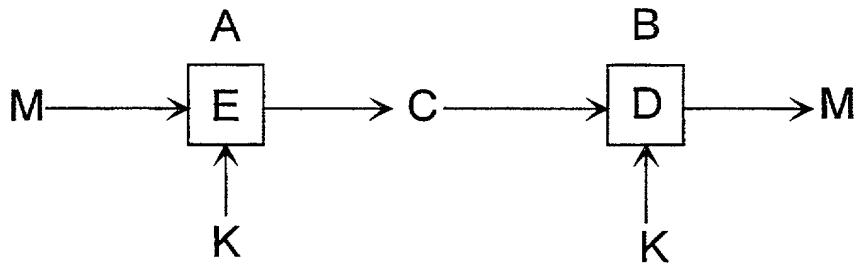


Fig. 1b

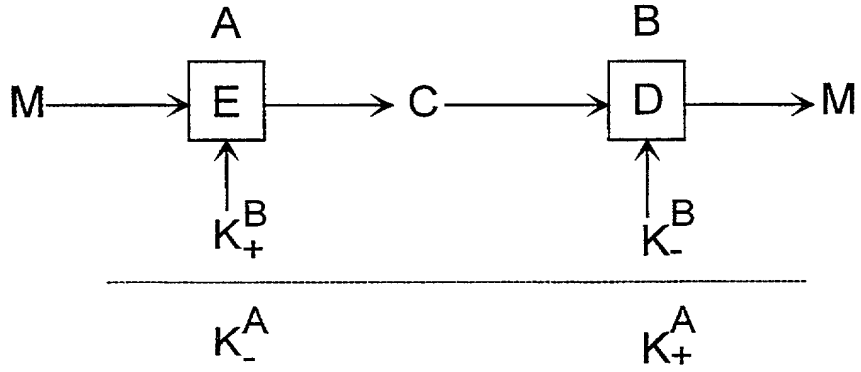


Fig. 2

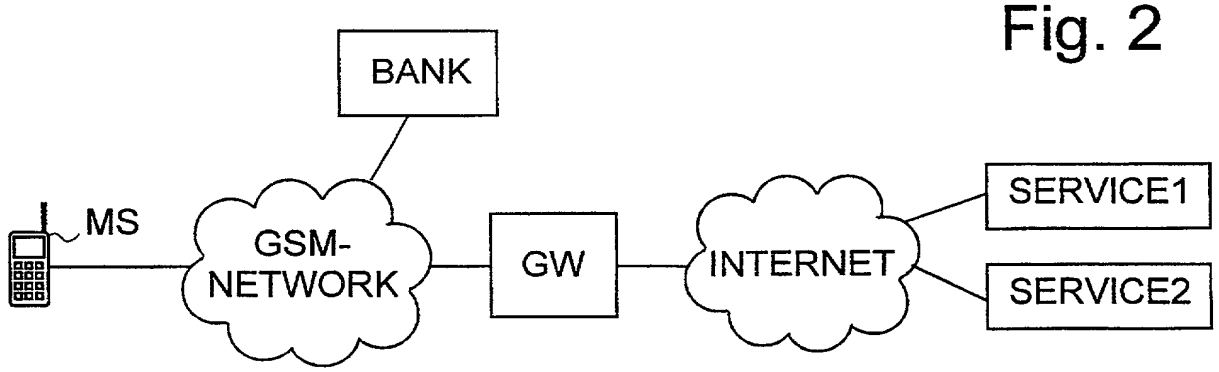


Fig. 3

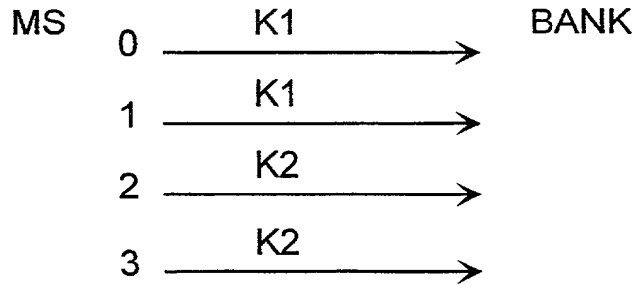
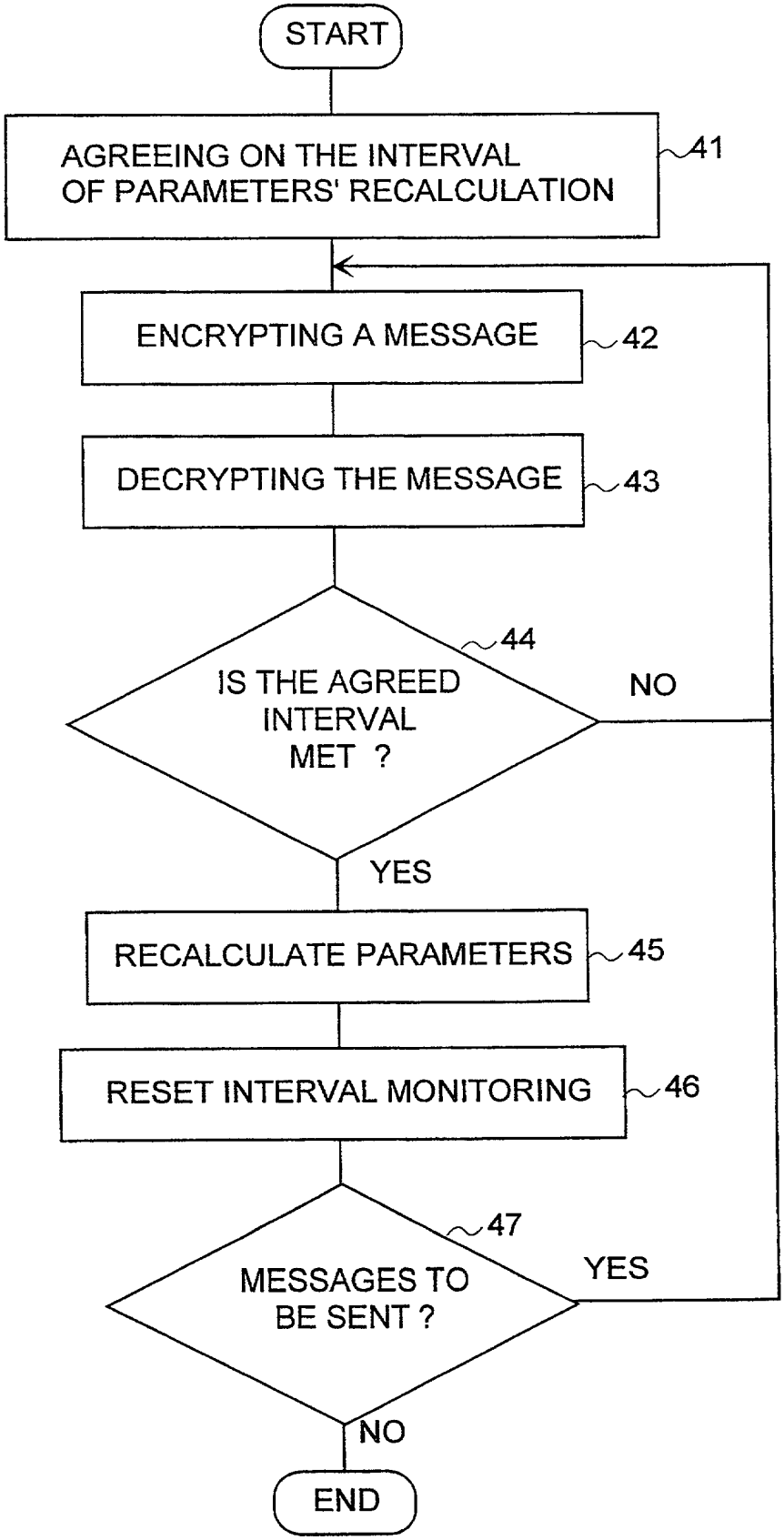


Fig. 4


START
AGREEING ON THE INTERVAL OF PARAMETERS' RECALCULATION
41
ENCRYPTING A MESSAGE
42
DECRYPTING THE MESSAGE
43
44
IS THE AGREED INTERVAL MET ?
NO
YES
RECALCULATE PARAMETERS
45
RESET INTERVAL MONITORING
46
47
MESSAGES TO BE SENT ?
YES
NO
END

Altera Reference No.: 796.337USW1

Altera Law Group, LLC

Declaration and Power of Attorney Patent Application (Design or Utility)

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled: SECURITY METHOD FOR TRANSMISSIONS IN TELECOMMUNICATION NETWORKS

the specification of which

☐ is referred to by Altera reference number on a separate document
☒ is attached hereto
☐ was filed on 9 March 2000 as application serial no. _____ and or PCT International Application number _____ and was amended on _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose to the U.S. Patent and Trademark Office all information know to me to be material to patentability as defined in 37 C.F.R.§1.56.

I hereby claim foreign priority benefits under 35 U.S.C.§119(a)-(d) or 35 U.S.C.§365(b) of any foreign application(s) for patent or inventor's certificate, or 35 U.S.C.§365(a) of any PCT International application which designated at least one country other than the United States, listed below and have also identified below any foreign application for patent or inventor's certificate of PCT International application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application(s)		
Number 973694	**Country** Finland	**Day/Month/Year Filed** 15 September 1997
Number	**Country**	**Day/Month/Year Filed**
Number	**Country**	**Day/Month/Year Filed**

I hereby claim the benefit under 35 U.S.C. §119(e) of any United States provisional application(s) listed below:

Prior Provisional Application(s)	
Serial Number	**Day/Month/Year Filing Date**
Serial Number	**Day/Month/Year Filing Date**
Serial Number	**Day/Month/Year Filing Date**

I hereby claim the benefit under 35 U.S.C. §120 of any United States application(s), or under 35 U.S.C. §365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of 35 U.S.C. §112, I acknowledge the duty to disclose to the U.S. Patent and Trademark Office all information known to me to be material to patentability as defined in 37 C.F.R.§1.56 which became available between the filing date of the prior application and the national or PCT International filing date of this application:

Prior U.S. or International Application(s)		
Serial Number PCT/FI98/00721	**Day/Month/Year Filed** 15 September 1998	**Status** (patented, pending, abandoned) Pending
Serial Number	**Day/Month/Year Filed**	**Status** (patented, pending, abandoned)
Serial Number	**Day/Month/Year Filed**	**Status** (patented, pending, abandoned)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements are made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C.§1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Altera Reference No.: 796.337US01

Power of Attorney

As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith.

Steven R. Funk	Reg. No. 37,830	David W. Lynch	Reg. No. 36,204
Michael B. Lasky	Reg. No. 29,555	Karen D. McDaniel	Reg. No. 37,674
Iain A. McIntyre	Reg. No. 40,337		

I hereby authorize them or others whom they may appoint to act and rely on instructions from and communicate directly with the person/organization who/which first sends this case to them and by whom/which I hereby declare that I have consented after full disclosure to be represented unless/until I instruct Altera Law Group, LLC otherwise.

Please direct all correspondence in this case to Altera Law Group, LLC at the address indicated below:

Michael B. Lasky
Altera Law Group, LLC
10749 Bren Road East, Opus 2
Minneapolis, MN 55343

Full Name of Sole or First Inventor		
Family Name Raivisto	**First Given Name** Tommi	**Second Given Name**
Residence and Citizenship		
City of Residence Helsinki	**State or Country of Residence** Finland	**Country of Citizenship** Finland
Post Office Address		
Street Address Liusketie 16 I 54	**City** FIN-00710 Helsinki	**State & Zip Code or Country** Finland
Signature of Inventor		**Date**